Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Use of Personal Email Accounts for Public Business

Introduction

This document explains the implications under the *Freedom of Information and Protection of Privacy Act* ("FIPPA") for use of personal email accounts for work purposes by employees of public bodies. It conveys two key messages. First, FIPPA applies to the use of personal email accounts for work purposes. Second, public bodies should not, for FIPPA purposes, allow the use of personal email accounts for work.

Application of FIPPA to Personal Email Accounts

FIPPA applies to all records in the custody *or* under the control of a public body. Email are records under FIPPA.[1] Records are in the custody of a public body if it has "charge and control" of the records, "including some legal responsibility for their safekeeping, care, protection or preservation."[2] While the public body would have custody of email residing on its server, it would not have custody for personal email residing elsewhere. The issue in such cases would be whether personal email is under the control of a public body.

The use of personal email accounts for work purposes can give the perception that public body employees are seeking to evade the freedom of information process.

The Supreme Court of Canada has said that where a record is not in the physical possession of a government institution, it will still be under its control if these two questions are answered in the affirmative:

---

[1] See s. 3(1) of FIPPA.

[2] See para. 23 of Order 02-30, [2002] B.C.I.P.C.D. No. 30 and p. 9 of Order No. 308-1999, [1999] B.C.I.P.C.D. No. 21.

(1) Do the contents of the document relate to a departmental matter?

(2) Could the government institution reasonably expect to obtain a copy of the document upon request?[3]

The facts of each case will determine whether personal email are under the control of a public body. As a general rule, any email that an employee sends or receives as part of her or his employment duties will be a record under the public body's control, even if a personal account is used.

ADEQUATE SEARCH (S. 6(1) OF FIPPA)

FIPPA requires public bodies to make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely. This includes a duty to perform an adequate search for records that respond to an access request. A public body must be able to prove that its search efforts have been thorough and comprehensive and that it has explored all reasonable avenues to locate records.[4] The Information and Privacy Commissioner has the authority to compel the production of records in the custody or under the control of a person[5], including those in personal email accounts.

The use of personal email accounts by employees does not remove or reduce the duty of a public body to search for records and produce those that are responsive to an access request.

The use of personal email accounts does not relieve public bodies of their duty to comprehensively search for requested records and to produce them. While nothing in FIPPA directly prohibits public body employees from using personal email accounts, doing so may make it more difficult for their employer to search for records. Employees may be unwilling to produce records from their personal account or to allow access to their accounts for that purpose.

To address this risk, public bodies should create policy on the use of personal email accounts for work purposes. A preferred solution is for public bodies to require the use of its email system for work purposes. If that is truly not practicable, the policy should be that employees must copy their work email account on any work-related email they send from a personal account.[6] This policy should be part of each employee's conditions of employment.

---

[3] See *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2011 SCC 25.
[4] See, for example, Order F07-12, [2007] B.C.I.P.C.D. No. 17, Order 00-32, [2000] B.C.I.P.C.D. No. 35 and Order 00-26, [2000] B.C.I.P.C.D. No. 29.
[5] See s. 44(1)(b) of FIPPA.
[6] This policy should also apply where there is a ban on use of personal email accounts for work purposes, to deal with cases where an employee failed to comply with the policy and possesses personal email that might be responsive to an access to information request.

REASONABLE SECURITY MEASURES (S. 30 OF FIPPA)

Another risk relates to security of personal information. FIPPA requires public bodies to take reasonable security measures to guard against unauthorized access, collection, use, disclosure or disposal of personal information. A personal email account, which is often web-based, is much less likely to comply with this requirement than a public body's email system. First, the terms of service for personal accounts may allow third-party access to content in a way that is in contravention of FIPPA. Second, security features for webmail services may not be adequate for FIPPA purposes. Any public body that allows use of personal email accounts to send or receive personal information is therefore risking non-compliance with FIPPA.

Storage and Access must be in Canada (s. 30.1 of FIPPA)

Although there are exceptions, including consent by affected individuals, [7] FIPPA requires public bodies to store and access personal information only in Canada. Public bodies have to assume that webmail resides on servers outside Canada, at least some of the time. This presents a serious risk of non-compliance for public bodies that allow use of personal email that contains personal information.

Disclosure Outside of Canada (s. 33.1 of FIPPA)

FIPPA prohibits the disclosure of personal information outside of Canada unless authorised by s. 33.1. The use of a webmail service that has servers outside of Canada will almost certainly result in public bodies disclosing personal information outside of Canada. Unless s. 33.1 authorizes the disclosure, use of webmail to send or receive personal information would violate FIPPA.

RESPONSIBLE INFORMATION MANAGEMENT

The citizens of British Columbia expect accountability from public bodies in their actions as well as their information practices. One important way for public bodies to demonstrate this accountability is to create an accurate record of actions in a manner that preserves records of enduring value. When employees of public bodies conduct business through their personal email accounts, accountability is easily lost.

[7] See s. 11(2)(b) of the Freedom of Information and Protection of Privacy Regulation. The rules for obtaining consent mean that public bodies will rarely be authorized to use personal email accounts.

CONCLUSION

FIPPA applies to work-related email sent to or received from the personal email accounts of public body employees. This document shows how use of personal email accounts for work purposes presents several challenges for public bodies under FIPPA. As indicated above, for FIPPA purposes, public bodies should not allow use of personal email accounts to conduct public business. They should ensure that clear policy is in place in this area and that all employees agree to comply with the policy.

If you have any questions about this document, please contact us at:

Office of the Information and Privacy Commissioner for BC
Tel: (250) 387-5629 (in Vancouver call (604) 660-2421)
Elsewhere in BC call 1-800-663-7867
Email: info@oipc.bc.ca